Quadratic Congruences

Paul Stoienescu and Tudor-Dimitrie Popescu

Abstract. In this note, we will present some olympiad problems which can be solved using quadratic congruences arguments.

1 Definitions and Properties

Let x, y and z be integers, $x > 1$, $y \geq 1$ and $(x, z) = 1$. We say that z is a residue of $y - th$ degree modulo x if congruence $n^y \equiv z \pmod{x}$ has an intenger solution. Otherwise z is a nonresidue of $y - th$ degree. For $x = 2, 3, 4$ the residues are called quadratic, cubic, biquadratic, respectively. This article is mainly focused on quadratic residues and their properties.

Lemma Let p be an odd prime. There are $\frac{p-1}{2}$ quadratic residues in the set $\{1, 2, 3..., p-1\}$.

1.1 Legendre's Symbol

Given a prime number p and an integer a, Legendre's symbol $\left(\frac{a}{p}\right)$ is defined as:

$$(\frac{a}{p}) = \begin{cases} 1 & \text{if a is a quadratic residue modulo p} \\ -1 & \text{otherwise} \end{cases} \tag{1}$$

Property 1 If $a \equiv b \pmod{p}$ and ab is not divisible by p, then $(\frac{a}{p}) = (\frac{b}{p})$.

Property 2 Legendre's symbol is multiplicative, *i.e.* $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ for all integers a, b and prime number $p > 2$.

Property 3 If $p \neq 2$, then $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$.

Property 4 If $p \neq 2$, then $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.

Property 5 If $p \not| a$, $p \neq 2$, then $a^{\frac{p-1}{2}} \equiv (\frac{a}{p}) \pmod{p}$ **(Euler's Criterion)**

Property 6 If p, q are distinct odd prime numbers, then $(\frac{p}{q}) = (\frac{q}{p}) \cdot (-1)^{\frac{(p-1)\cdot(q-1)}{4}}$ **(Quadratic Reciprocity Law of Gauss)**

1.2 Quadratic Congruences to Composite Moduli

Let a be an integer and b an odd number, and let $b = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ be the factorization of b into primes. Jakobi's Symbol $(\frac{a}{b})$ is defined as:

$$(\frac{a}{b}) = (\frac{a}{p_1})^{\alpha_1} (\frac{a}{p_2})^{\alpha_2} \dots (\frac{a}{p_n})^{\alpha_n} \tag{2}$$

Jakobi's Symbol has almost the same properties as Legendre's with few modifications: It doesn't have property 5, while at properties 3 and 4 p is changed with an odd integer and at property 6 p, q are changed with distinct odd integers with no common divisors.
It is easy to see that $(\frac{a}{b}) = -1$ implies that a is a quadratic nonresidue $\pmod{p}$. Indeed, if $(\frac{a}{b}) = -1$, then by definition $(\frac{a}{p_i}) = -1$ for at least one $p_i | b$; hence a is a quadratic nonresidue modulo p_i. The converse is false as seen from the example $(\frac{2}{15}) = (\frac{2}{3})(\frac{2}{5}) = (-1)(-1) = 1$ but 2 is not a quadratic residue modulo 15.

Theorem Let a be an integer and b be a positive integer, and let $b = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ be the factorization of b into primes. Then a is a quadratic residue modulo b if and only if a is a quadratic residue modulo $p_i^{\alpha_i}$, for each $i = 1, 2, \dots n$.

2 Warm-Up Problems

2.1

1.The positive integers a and b are such that the numbers $15a+16b$ and $16a-15b$ are both squares of positive integers. What is the least possible value that can be taken on by the smaller of these two squares?

Solution Let $15a+16b = k^2$ and $16a-15b = l^2 \Rightarrow a = \frac{15k^2+16l^2}{481}$, $b = \frac{16k^2-15l^2}{481}$, $k, l \in N^*$. $481 = 13 \cdot 37 \Rightarrow 15k^2+16l^2 \equiv 0 \pmod{13}$, $2k^2 \equiv -3l^2 \pmod{13}$, $k^2 \equiv 5l^2 \pmod{13}$. We have $(\frac{5}{13}) = -1 \Rightarrow 13|l, 13|k$. $15k^2+16l^2 \equiv 0 \pmod{37}$, $32l^2 \equiv -30k^2 \pmod{37}$, $-5l^2 \equiv -30k^2 \pmod{37}$, $l^2 \equiv 6k^2 \pmod{37}$. Combined with the fact that $(\frac{6}{37}) = -1$ we get that $37|k$, $37|l$. The least possible value for l is $13 \cdot 37 = 481$. We can take $k = l = 481$ and thus we'll get $a = 31 \cdot 481$, $b = 481$.

2.2

Prove that 2^n+1 has no prime factors of the form $8k+7$. (Vietnam team selection test 2004)

Solution Assume that there exists a prime p such that $p|2^n+1$ and $p \equiv 7 \pmod 8$. If n is even, then $(\frac{-1}{p}) = 1$ but $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = -1$ because $p \equiv 3 \pmod 4$, a contradiction. If n is odd, then $(\frac{-2}{p}) = 1$ but $(\frac{-2}{p}) = (-1)^{\frac{p^2-1}{8}} \cdot (-1)^{\frac{p-1}{2}} = -1$ again a contradiction due to the fact that $p \equiv 7 \pmod 8$.

2.3

Let p a prime number greater than 3. Calculate:

a)$S = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{2k^2}{p}\right] - 2 \cdot \left[\frac{k^2}{p}\right]$ if $p \equiv 1 \mod 4$

b) $T = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{k^2}{p}\right]$ if $p \equiv 1 \mod 8$

Solution $a)$Let $r_1, r_2 ... r_{\frac{p-1}{2}}$ be the quadradic residues $\pmod p$ First, let's observe that the sum is equivalent to $\sum_{i=1}^{\frac{p-2}{2}} 2\{\frac{r_i}{p}\} - \{\frac{2r_i}{p}\}$. Each term $2\{\frac{r_i}{p}\} - \{\frac{2r_i}{p}\}$ is 0 if $r_i \leq \frac{p-1}{2}$ and 1 if $r_i > \frac{p-1}{2}$. So S is the number of quadratic residues which are greater than $\frac{p-1}{2}$. Since $p \equiv 1 \pmod 4 \Rightarrow$ if r_i is quadratic residue , then so is $p - r_i$, so there are half quadratic residues which are greater than $\frac{p-1}{2}$ $\Rightarrow S = \frac{p-1}{4}$.

$b)$ We have $T = \frac{\sum_{k=1}^{\frac{p-1}{2}} [\frac{2k^2}{p}] - S}{2}$ so all we have to do is to calculate $\sum_{k=1}^{\frac{p-1}{2}} [\frac{2k^2}{p}]$ which is equivalent to $\frac{2(1^2+2^2+... \frac{(p-1)^2}{4}) - (r_1+r_2+...r_{\frac{p-1}{2}})}{p}$ where $r_1, r_2, ... r_{\frac{p-1}{2}}$ are the quadratic residues $\pmod p$. This is because 2 is a quadratic residue $\pmod p$. From now on it's easy because $r_1 + r_2 + ... r_{\frac{p-1}{2}} = \frac{p(p-1)}{4}$ (remember that $p \equiv 1 \pmod 4$ means that if r_i is a quadratic residue, then so is $p - r_i$).

2.4

Let $m,\ n \geq 3$ be positive odd integers. Prove that $2^m - 1$ doesn't divide $3^n - 1$.

Solution Here we will use Jacoby's Symbol. Suppose that $2^m - 1$ divides $3^n - 1$. Let $x = 3^{\frac{n-1}{2}}$. We have $3x^2 \equiv 1 \pmod{2^m - 1}$ so $(3x)^2 \equiv 3 \pmod{2^m - 1} \Rightarrow (\frac{3}{2^m-1}) = 1$. Using quadratic reciprocity, $1 = (\frac{3}{2^m-1}) = (\frac{2^m-1}{3})(-1)^{\frac{2^m-2}{2}} \Rightarrow (\frac{2^m-1}{3}) = -1$ and this is a contradiction due to the fact that $2^m - 1 \equiv 1 \pmod 3$.

3 Harder Problems

3.1 2013 Romanian Master in Mathematics

For a positive integer a, define a sequence of integers $x_1, x_2, \dots$ by letting $x_1 = a$ and $x_{n+1} = 2x_n + 1$ for $n \geq 1$. Let $y_n = 2^{x_n} - 1$. Determine the largest possible k such that, for some positive integer a, the numbers $y_1, \dots, y_k$ are all prime.

Solution We will prove that the answer is 2. Suppose that there exists a such that $k \geq 3$. The numbers $2^a - 1$, $2^{2a+1} - 1$, $2^{4a+3} - 1$ are primes $\Rightarrow$ the numbers $a, 2a+1, 4a+3$ are primes (this is because of the fact that if $2^M - 1$ is prime, then M is also a prime. Otherwise if there existed a natural number d such that $d|M$ then $2^d - 1$ would divide $2^M - 1$). Let's use Euler's Criterion. $2^{\frac{4a+3-1}{2}} \equiv (\frac{2}{4a+3}) \pmod{4a+3} \Rightarrow 2^{2a+1} \equiv (\frac{2}{4a+3}) \pmod{4a+3}$. $2^{2a+1} - 1$ is prime so $2^{2a+1} \not\equiv 1 \pmod{4a+3}$, otherwise $2^{2a+1} = 4a+4$ and that will lead to $a = 1$, false. Hence we have $(\frac{2}{4a+3}) = -1 \Rightarrow -1 = (-1)^{\frac{(4a+2)(4a+4)}{8}} = (-1)^{(2a+1)(a+1)} \Rightarrow a+1$ is odd but a is prime so $a = 2$. If $a = 2$ we have that $2^{11} - 1 = 23 \cdot 87$ is not prime, contradiction. So we get that the answer is 2 and it's achieved for $a = 2$.

3.2 2004 Romanian IMO Team Selection Test

Let p be an odd prime, a_i, $i = 1, 2 \dots p-1$ be Legendre's symbol of i relative to p (i.e. $a_i = 1$ if $i^{\frac{p-1}{2}} \equiv 1$ and $a_i = -1$ otherwise). Consider the polynomial:
$f = a_1 + a_2 X + \dots a_{p-1} X^{p-2}$.
a) Prove that 1 is a simple root of f if and only if $p \equiv 3 \pmod 4$.
b) Prove that if $p \equiv 5 \pmod 8$, then f is a root of f of order exactly 1.

Solution a) We have that $f(1) = \displaystyle\sum_{j=1}^{p-1} (\frac{j}{p}) = 0$ because there are $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ nonquadratic residues modulo p. Suppose $p \equiv 1 \pmod 4$. Let's show that $f'(1) = 0$. $f'(1) = a_2 + 2a_3 + 3a_4 + \dots + (p-2)a_{p-1}$, $(\frac{-1}{p}) = 1 \Rightarrow a_j = a_{p-j}$ so $(j-1)a_j + (p-j+1)a_{p-j} = (p-2)a_j$ and $f'(1) = (p-2)\displaystyle\sum_{j=1}^{\frac{p-1}{2}} a_j$. Denote $S = \displaystyle\sum_{j=1}^{\frac{p-1}{2}} a_j$ and $T = \displaystyle\sum_{i=\frac{p+1}{2}}^{p-1}$. $S + T = 0$ and $S = T$ (because $a_j = a_{p-j}$) $\Rightarrow S = T = 0 \Rightarrow f'(1) = (p-2)S = 0$ and 1 is not a simple root of f. Let's suppose now that $p \equiv 3 \pmod 4$. $(\frac{-1}{p}) = -1 \Rightarrow a_j = -a_{p-j+1} \Rightarrow (j-1)a_j + (p-j-1)a_{p-j} = a_j(2j-p)$ is an odd number $\Rightarrow f'(1) = \displaystyle\sum_{j=1}^{\frac{p-1}{2}} a_j(2j-p)$ is odd (because $\frac{p-1}{2}$ is odd) , so $f'(1) \neq 0$ and 1 is a simple root of f.

$b)$ Let p be a prime, $p \equiv 4 \pmod 8$. We've already proved that $f'(1) = 0$. To solve the problem , it is enough to prove that $f"(1) = \sum_{j=1}^{p-1}(j-2)(j-1)a_j \neq 1$ and for this we will show that $f"(1) \equiv 4 \pmod 8$. $a_j = a_{p-j}$ ($(\frac{-1}{p}) = 1) \Rightarrow (j-2)(j-1)a_j+(p-j-2)(p-j-1)a_{p-j} \equiv a_j[(j-2)(j-1)+(3-j)(4-j)] = a_j(j^2-3j+2+j^2-7j+12 \equiv a_j(2j^2-2j-2) \pmod 8$. It's easy to show that $2j^2-2j-2 \equiv 2 \pmod 8$ if $j \equiv 2, 3 \pmod 4$ and $2j^2-2j-2 \equiv -2 \pmod 8$ if $j \equiv 0, 1 \pmod 4$. So $f"(1) \equiv 2(-a_1+a_2+a_3-a_4 \cdots + a_{4k-1}-a_{4k}-a_{4k+1}+a_{4k+2}) \pmod 8$ where $p = 8k+5$. We know from $a)$ that $\sum_{j=1}^{\frac{p-1}{2}} a_j = 0$ if $p \equiv 1 \pmod 4 \Rightarrow f"(1) \equiv 4(a_2+a_3+a_6+a_7+\ldots a_{4k-1}+a_{4k+2}) \pmod 8$ but the sum $a_2+a_3+a_6 \ldots a_{4k+2}$ is odd (it's the sum of $2k+1$ odd numbers) so $f"(1) \equiv 4 \pmod 8$ and we've finished.

3.3 IMO 2008

Prove that there are infinitely many positive integers n such that n^2+1 has a prime divisor greater than $2n+\sqrt{2n}$

Solution Let p be a prime, $p = 8k+1$. Note that $4^{-1} \equiv 6k+1 \pmod p$. Choose $n = 4k-a$, $0 \leq a < 4k$. Then $(\frac{p-1}{2}-a)^2+1 \equiv 0 \pmod p$ is equivalent to $4^{-1}+a+a^2+1 \equiv 0 \pmod p$, so $a(a+1) \equiv -6k-2 \equiv 2k-1 \pmod p$. But $a(a+1)$ is even and positive, so $a(a+1) \geq 10k$. We have that $(a+1)^2 > a(a+1) \geq 10k > p$, so $n = \frac{p+1}{2}-(a+1) < \frac{p+1}{2}-\sqrt{p} < \frac{p+1}{2}-\sqrt{2n}$, so $2n+2\sqrt{2n}-1 > p$. Note that this result is a bit stronger than the initial inequality.

3.4 2005 Moldavian IMO Team Selection Test

Given functions $f, g : N^* \to N^*$, g is surjective and $2f(n)^2 = n^2+g(n)^2$, $\forall n > 0$. Prove that if $|f(n)-n| \leq 2005\sqrt{n}$, $\forall n > 0$, then $f(n) = n$ for infinitely many n.

Solution It's easy (by Dirichlet's Theorem) to find a strictly increasing sequence of prime numbers p_n with $p_n \equiv 3 \pmod 8$. Because g is surjective, there is a sequence a_n with $g(a_n) = p_n$. We have $2f(a_n)^2 = a_n^2+p_n^2 \Rightarrow 2f(a_n)^2 \equiv a_n^2 \pmod{p_n}$ and because $(\frac{2}{p_n}) = -1 \Rightarrow p_n|a_n$ and $p_n|f(a_n)$ so there exist sequences x_n and y_n such that $a_n = x_n p_n$ and $f(a_n) = y_n p_n$. We have $2y_n^2 = x_n^2+1$ and $|\frac{f(a_n)}{a_n}-1| \leq \frac{2005}{\sqrt{a_n}} \Rightarrow \lim_{n\to\infty} \frac{f(a_n)}{a_n} = 1 \Rightarrow \lim_{n\to\infty} \frac{\sqrt{x_n^2+1}}{x_n} = \sqrt{2} \Rightarrow \lim_{n\to\infty} x_n = \lim_{n\to\infty} y_n = 1$ and because x_n and y_n are integers sequences $\Rightarrow$ there exists a number k for which $x_n = y_n = 1$ and $f(p_n) = p_n$,for every $n \geq k$, hence the conclusion follows.

3.5 2013 Iran Team Selection Test

Do there exist natural numbers a, b and c such that $a^2 + b^2 + c^2$ is divisible by $2013(ab + bc + ca)$?

Solution Suppose that exists n such that $a^2 + b^2 + c^2 = 2013n(ab + bc + ac) \Rightarrow (a + b + c)^2 = (2013n + 2)(ab + bc + ac)$. Choose a prime p with $p \equiv 2 \pmod 3$ which divides $2013n+2$ with an odd exponent($p^{2i+1}||2013n+2$ for some positive integer i). Then $p^{i+1}|a+b+c$ and therefore $p|a+b+c$. Because $p|ab+bc+ac \Rightarrow p|a^2+ab+b^2$ (this is easy by substituting $c \equiv -a - b \pmod p$)$\Rightarrow p|(2a+b)^2+3b^2$ $\Rightarrow (\frac{-3}{p}) = 1$ but this is false, so there are no such triplets.

3.6 A very useful lemma

Suppose that the positive integer a is not a perfect square. Then $(\frac{a}{p}) = -1$ for infinitely many primes p.

Solution Let's say that it's not true. This means that there exists a number r such that for every prime $q > r$, $(\frac{a}{q}) = 1$. Because a is not a perfect square, we can write $a = x^2 p_1 p_2 ... p_k$ where $p_1, p_2 ... p_k$ are primes in increasing order. Let's take a prime $p > r$, $p \equiv 5 \pmod 8$. We have that $(\frac{a}{p}) = (\frac{p_1}{p})(\frac{p_2}{p})...(\frac{p_k}{p})$. If p_i is odd, $(\frac{p_i}{p}) = (\frac{p}{p_i})$ (from Quadratic Reciprocity Law). If $p_1 = 2$, $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = -1$. $(\frac{a}{p}) = (\frac{p}{p_1})...(\frac{p}{p_k})$ or $(\frac{a}{p}) = -(\frac{p}{p_2})...(\frac{p}{p_k})$. We can take $r_2, r_2, ..., r_k$ residues $\pmod{p_2, p_3 ... p_k}$ such that $(\frac{r_2}{p_2})...(\frac{r_k}{p_k})$ is 1 or -1 as we wish. By Chinese Remainders Theorem there are infinitely numbers t with $t \equiv 5 \pmod 8$,$t \equiv r_i \pmod{p_i}$, $2 \leq i \leq k$. Now we look at progression $t + l8p_2p_3...p_k$. By Dirichlet's Theorem there are infinitely many prime q in this sequence and we take $q > r$. We have that $(\frac{a}{q}) = 1$ but as we've already discussed we can select $r_2, r_3 ... r_k$ such that $(\frac{a}{q}) = -1$, contradiction.

3.7 2015 Iran Team Selection Test

Let $b_1 < b_2 < b_3 < \dots$ be the sequence of all natural numbers which are sum of squares of two natural numbers. Prove that there exists infinite natural numbers like m which $b_{m+1} - b_m = 2015$.

Solution For any i , $1 \leq i \leq 2014$ we can find infinitely many primes p such that $p \equiv 3 \pmod 8$ and $(\frac{1007^2+i}{p}) = -1$ ($1007^2 + i$ is not a perfect square, so the second part follows easily from problem 6 and first part follows from Chinese Remainders Theorem and Dirichlet's Theorem). Now, we choose prime numbers $p_1, p_2 ..., p_{2014}$ such that $p_i \equiv 3 \pmod 8$ and $(\frac{1007^2+i}{p_i}) = -1$. There is a number x such that $x \equiv p_i - i \pmod{p_i^2}$ for any $1 \leq i \leq 2014$ (by Chinese Remainders Theorem). We will prove that there are infinitely many numbers a

such that the number $a^2 + 1007^2$ is of the form $x + kp_1^2p_2^2...p_{2014}^2$ for some k. If we note $y = a^2 + 1007^2$, we see that y and $y + 2015$ can be written as sum of squares of two natural numbers and $y + i$, $1 \leq i \leq 2014$, cannot because $y + i \equiv p_i \pmod{p_i^2}$. To prove this, we see that $(\frac{x-1007^2}{p_i}) = 1$, so there is a number x_i with $x_i^2 \equiv x - 1007^2 \pmod{p_i}$. We can find a numbers t_i such that $p_i^2|(x_i + p_i t_i)^2 - (x - 1007^2)$ (this is equivalent to finding a number t_i such that $p_i|\frac{x_i^2-x+1007^2}{p_i} + 2x_i t_i$ and that's easy because p_i does not divide x_i, otherwise p_i would divide $x - 1007^2$ and p_i would divide $1007^2 + i$ and we can avoid this by choosing p_i very large). We denote by r_i the residue of $x_i + p_i t_i \pmod{p_i^2}$. By Chinese Remaindes Theorem we can find infinitely many numbers a such that $a \equiv r_i \pmod{p_i^2}$, $1 \leq i \leq 2014$, this means that $a^2 \equiv x - 1007^2 \pmod{p_i^2}$, $1 \leq i \leq 2014 \Rightarrow a^2 + 1007^2 = x + kp_1^2p_2^2...p_{2014}^2$ for some k and that's all.

3.8 2013 Romanian Team Selection Test

Let S be the set of all rational numbers expressible in the form

$$\frac{(a_1^2 + a_1 - 1)(a_2^2 + a_2 - 1)\dots(a_n^2 + a_n - 1)}{(b_1^2 + b_1 - 1)(b_2^2 + b_2 - 1)\dots(b_n^2 + b_n - 1)}$$

for some positive integers $n, a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n$. Prove that there is an infinite number of primes in S.

Solution Clearly, S is closed under multiplication and division: if r and s are in S, so are rs and $\frac{r}{s}$. Any prime number which is 0, 1 or 4 (mod 5) is in S. $2^2 + 2 - 1 = 5$ so 5 is in S. Now we will prove by induction that every prime number which 1 or 4 $\pmod 5$ is in S ($11 = 3^2 + 3 - 1$ and $19 = 4^2 + 4 - 1$). Let's denote by $p_1, p_2, ..$ the sequence of primes of this form in increasing order, and let's say that $p_1, p_2...p_{n-1}$ are in S. We will show that p_n is also in S. Because 5 is a quadratic residue $\pmod{p_n}$ there is a number x such that $p_n|(2x + 1)^2 - 5$ $\Rightarrow p_n|x^2 + x - 1$ and we can choose x such that $2x + 1 < p_n \Rightarrow p_n^2$ does not divide $x^2 + x - 1$ and every prime which divides $x^2 + x - 1$ (every prime which divides $x^2 + x - 1$ is $0, 1, 4 \pmod 5$) is less than p_n. Because $x^2 + x - 1$ is product of primes which are among $p_1, p_2...p_n$ it can be written as tp_n where t is in $S \Rightarrow$ p_n is in S ($p_n = \frac{x^2+x-1}{t}$ and $\frac{x^2+x-1}{1^2+1-1} = x^2 + x - 1$ is in S) so the induction step is proved.

4 Some applications to Mordell's equation

$y^2 = x^3 + k$, where k is an integer is called Mordell's equation, because he proved in 1922 that this equation has finitely many integral solutions. Although at first sight it may seem that quadratic residues aren't useful in this particular equation, we'll see that this surely isn't the case.

4.1

The equation $y^2 = x^3 + 7$ has no integral solutions. If x is even, then $y^2 \equiv 7 \pmod 8$, false. This means that x is odd. Rewrite the equation as follows: $y^2 + 1 = x^3 + 8$, so $y^2 + 1 = (x + 2)(x^2 - 2x + 4)$. Since x is odd, we get that $x^2 - 2x + 4 = (x - 1)^2 + 3 \equiv 3 \pmod 4$. So there exists a prime p such that $p | x^2 - 2x + 4 \Rightarrow p | y^2 + 1 \Rightarrow -1 \equiv y^2 \pmod p$, so -1 is a quadratic residue ($\bmod\ p$), false, since $p \equiv 3 \pmod 4$.

4.2

The equation $y^2 = x^3 - 5$ has no integral solutions. Reducing mod 4, we get that y is even and $x \equiv 1 \pmod 4$. Rewrite the equation as $y^2 + 4 = x^3 - 1 = (x - 1)(x^2 + x + 1)$. Since $x \equiv 1 \pmod 4$, we get that $x^2 + x + 1 \equiv 3 \pmod 4$, so there exists a prime p such that $p | x^2 + x + 1$, so $p | y^2 + 4$. It follows that -4 is a quadratic residue $\pmod p$, contradiction, since $(\frac{-4}{p}) = (\frac{-1}{p})(\frac{4}{p}) = -1$.

5 Proposed problems

5.1

Let $p \geq 3$ be a prime number. Prove that the least quadratic nonresidue $\pmod p$ is less than $\sqrt{p} + 1$.

5.2

Let p be a prime number such that $p \equiv 1 \pmod 4$. Prove that the equation $x^p + 2^p = p^2 + y^2$ doesn't have any solutions in natural numbers.

5.3 2005 Romanian Team Selection Test

Let $n \geq 0$ be an integer and let $p \equiv 7 \pmod 8$ be a prime number. Prove that

$$\sum_{k=1}^{p-1} \left\{ \frac{k^{2^n}}{p} - \frac{1}{2} \right\} = \frac{p-1}{2}.$$

5.4 Mathematical Reflections

Let p be a prime of the form $4k+1$ such that $2^p \equiv 2 \pmod{p^2}$. Prove that there is a prime number q, divisor of $2^p - 1$, such that $2^q > (6p)^p$.

5.5 Mathematical Reflections

If m is a positive integer show that $5^m + 3$ has neither a prime divisor of the form $p = 30k + 11$ nor of the form $p = 30k - 1$.

5.6 2013 Tuymaada International Olympiad, Junior League, A. Golovanov

Solve the equation $p^2 - pq - q^3 = 1$ in prime numbers.

5.7

Solve in natural numbers: $10^n + 89 = x^2$.

5.8 (Mathematical Reflections)

Let a be a positive integer such that for each positive integer n the number $a+n^2$ can be written as a sum of two squares. Prove that a is a square.

5.9 2007 Bulgaria team selection test

Let $p = 4k + 3$ be a prime number. Find the number of different residues $\pmod{p}$ of $(x^2 + y^2)^2$, where $(x, p) = (y, p) = 1$

5.10 1999 Balkan Mathematical Olympiad

Let p be an odd prime congruent to 2 modulo 3. Prove that at most $p - 1$ members of the set $\{m^2 - n^3 - 1 \mid 0 < m,\ n < p\}$ are divisible by p.

5.11

Let q be an odd prime and r a positive integer such that q does not divide r, $r \equiv 3 \pmod{4}$ and $(\frac{-r}{q}) = 1$. Prove that $4qk + r$ does not divide $q^n + 1$ for any k, n positive integers.

References

1. Dusan Djukic: Quadratic Congruences, www.imocompedium.com
2. Titu Andreescu and Dorin Andrica. Number Theory: Structures,Examples and Problems. Springer, 2009
3. Keith Conrad:Examples of Mordell's Equation:http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/mordelleqn1.pdf
4. Xu Jiagu.Lecture Notes on Mathematical Olympiad Courses, For Senior Section, Volume 2, World Scientific
5. http://www.artofproblemsolving.com
6. Titu Andreescu. Mathematical Reflections, the first two years. XYZ Press, 2011
7. Laurentiu Panaitopol and Alexandru Gica. Probleme de aritmetica si teoria numerelor.Idei de rezolvare, Editura Gil